Attribute-based Access Control Architectures with the eIDAS Protocols

SSR 2016

Frank Morgner (Bundesdruckerei)
Paul Bastian (Bundesdruckerei)
Marc Fischlin (TU Darmstadt)

German electronic identity card

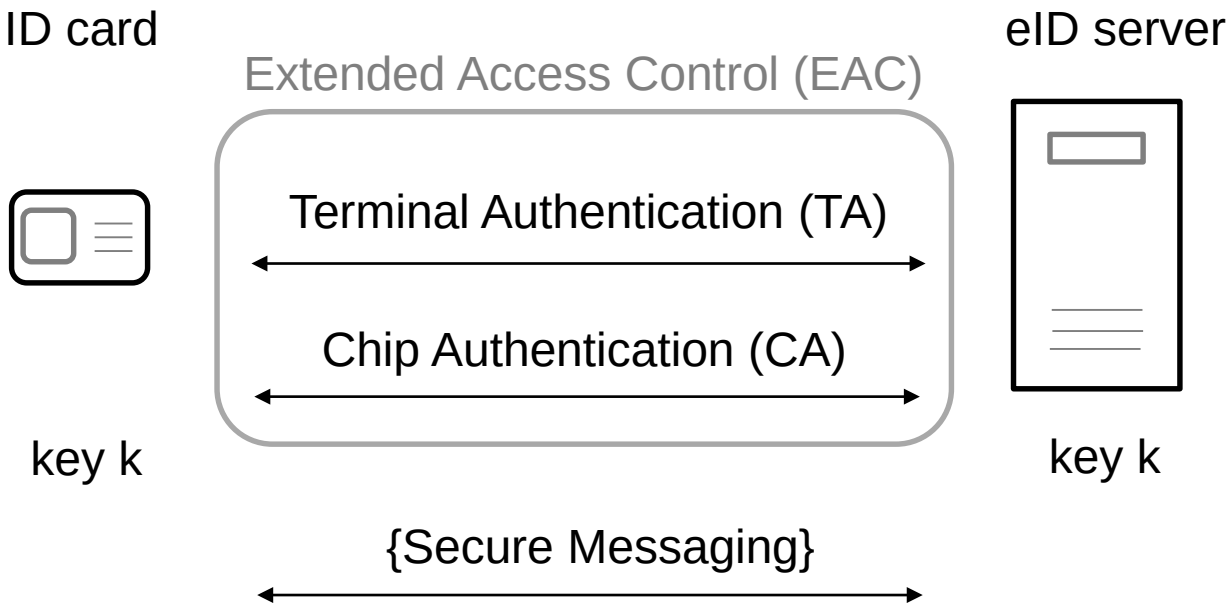
since November 2010

Cryptographic protocols of German identity card:

- also used for machine readable travel documents (ICAO Doc 9303)
- candidate for European eIDAS protocol

  electronic identification, authentication, and trust services for electronic transactions

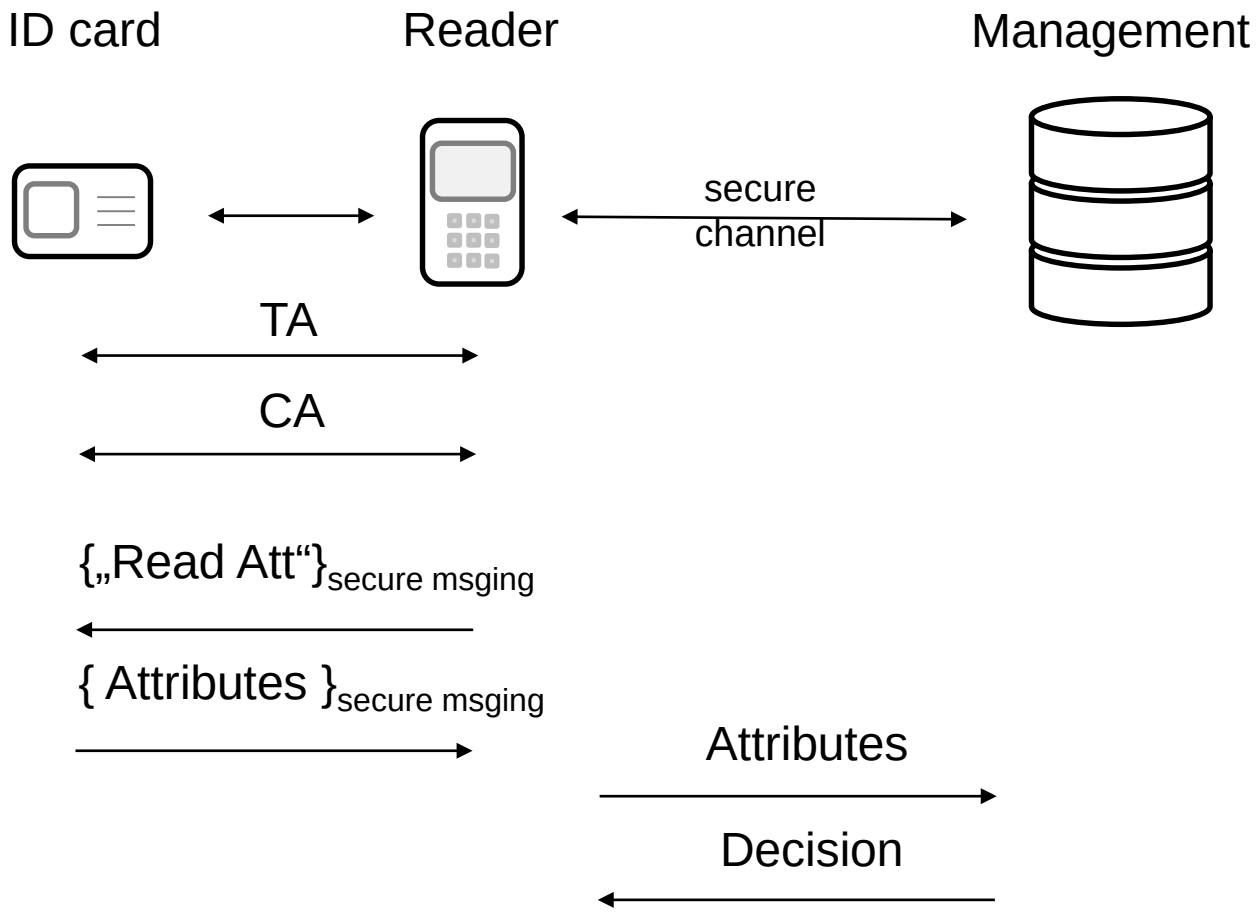
Basic Setting of German eID card



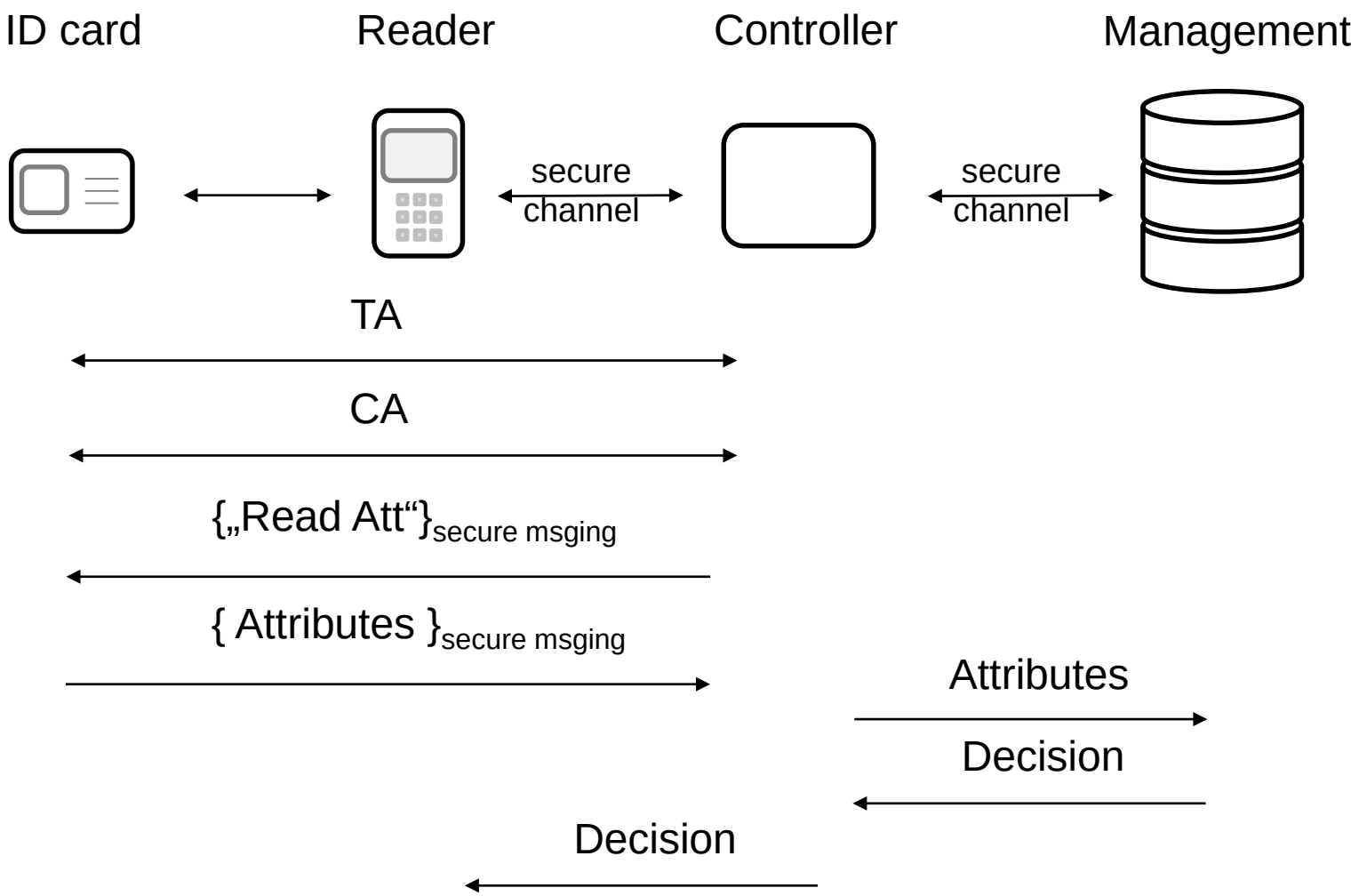
Secure extension to
attribute-based access control
in different scenarios?

Architectures

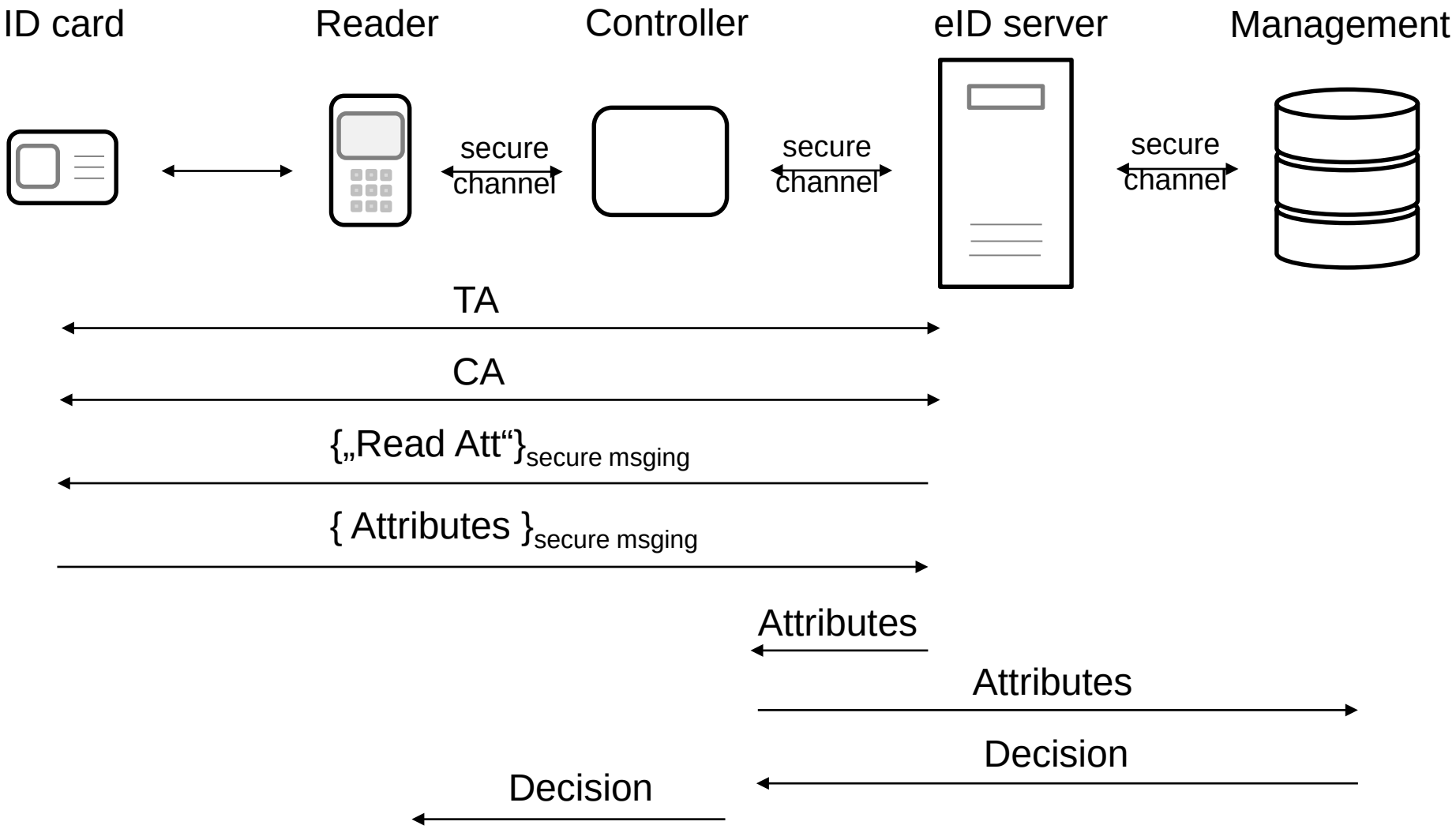
Integrated Architecture



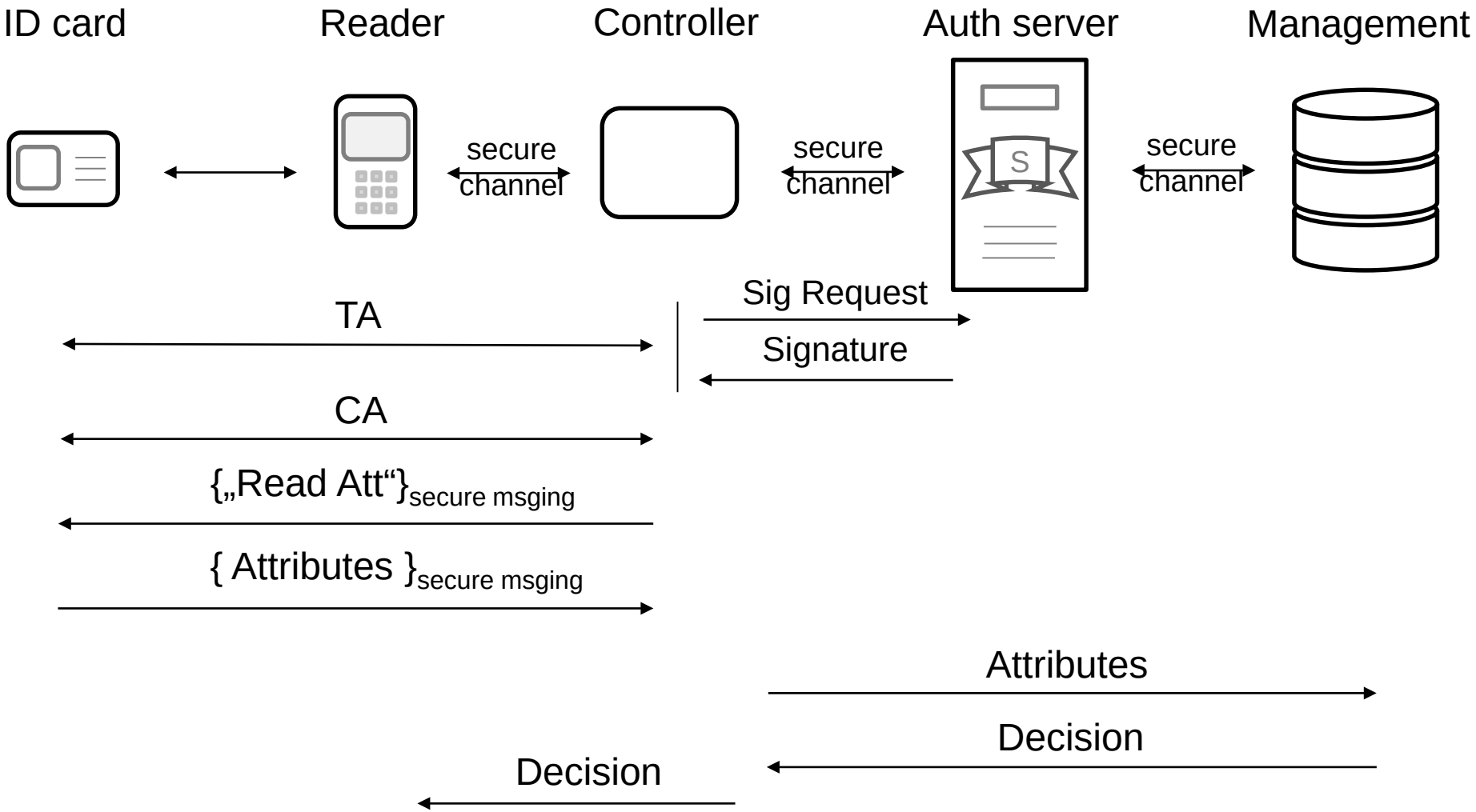
Distributed Architecture



eID-Service Architecture

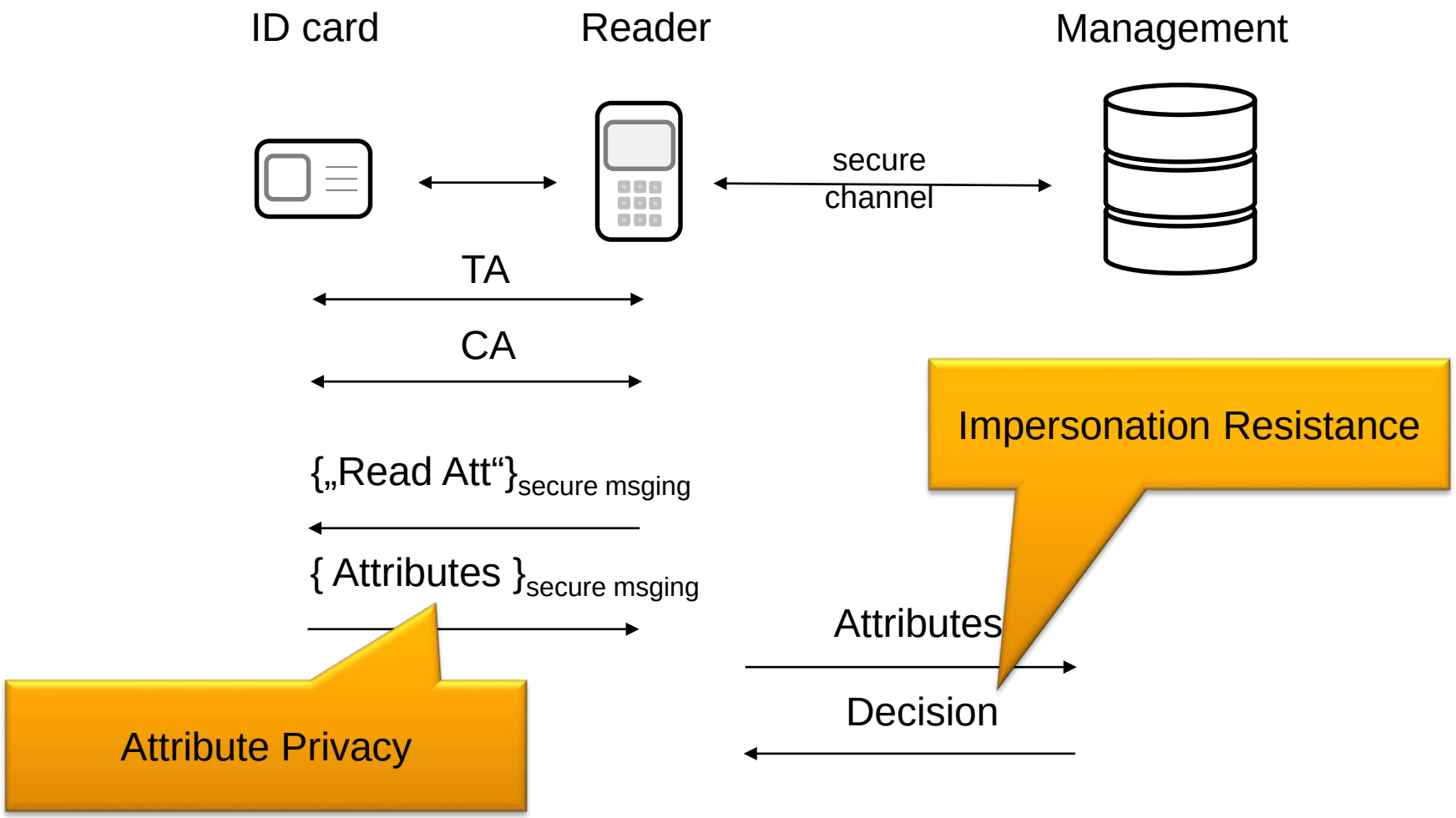


Authentication-Service Architecture

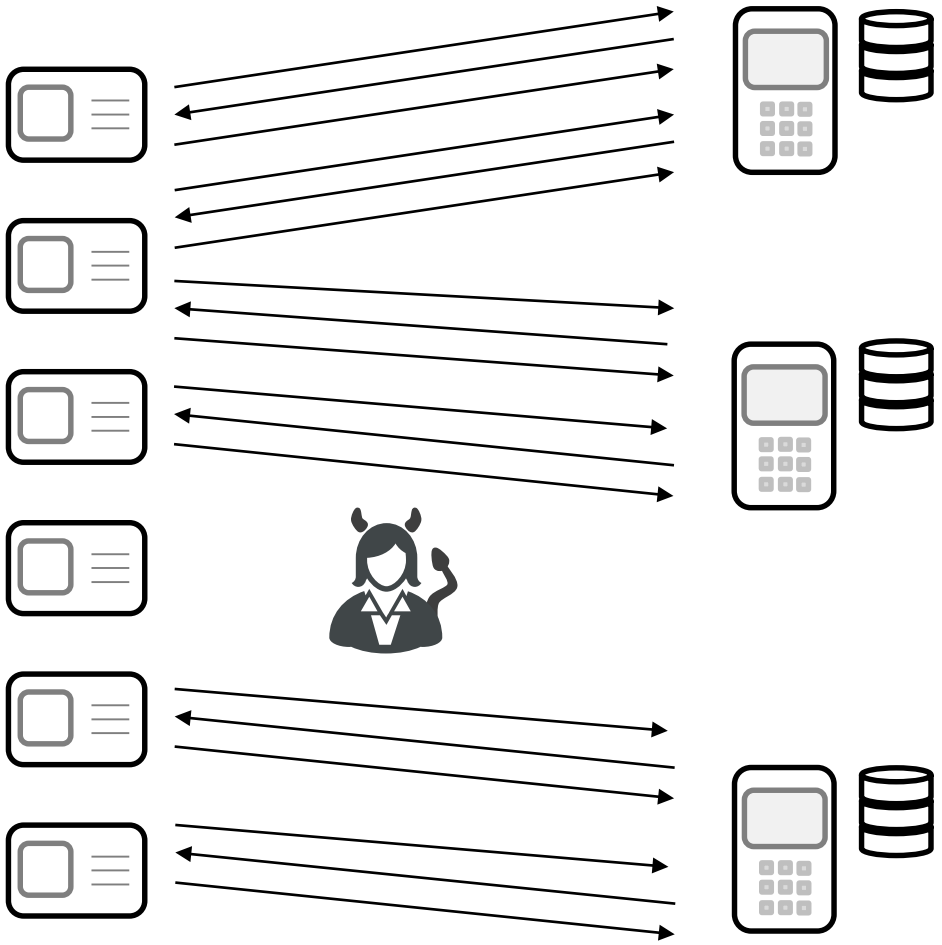


Security

Goals for Integrated Architecture



Dolev-Yao adversary (for both properties)



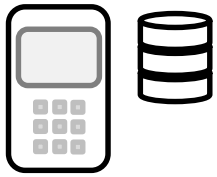
adversary can:

- eavesdrop
- inject/modify messages
- determine schedule
- corrupt parties
- determines data T

requires some notion of sessions and session identifiers

EAC Protocol

session identifier
$SID=(nonce_C, Compr(epk))$



certified key pair sk_C, pk_C

certified key pair sk_S, pk_S

pk_S, $certificate_S$ ←

pick ephemeral esk, epk

Compr(epk) ←

pick $nonce_C$

$nonce_C$ →

$s \leftarrow Sig(sk_S, nonce_C || Compr(epk))$

s ←

terminal authentication

chip authentication

pk_C, $certificate_C$ →

epk ←

pick $nonce^*_C$
$K = KDF(DH(sk_C, epk)\ nonce^*_C)$
$tag = MAC(K, epk)$

tag, $nonce^*_C$ →

$K = KDF(DH(epk, pk_C)\ nonce^*_C)$
verify tag

partner through certificate

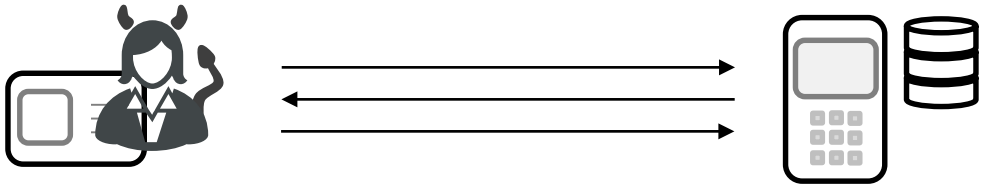
Defining security: impersonation resistance

(a) If party accepts in session SID for partner and attributes A,
then partner also accepts SID and A in some session

(b) at most two SIDs collide, one at a card, one at a reader

Example: „passive security“

formalized in common game-based style



pretends to be card

accepts with SID and A

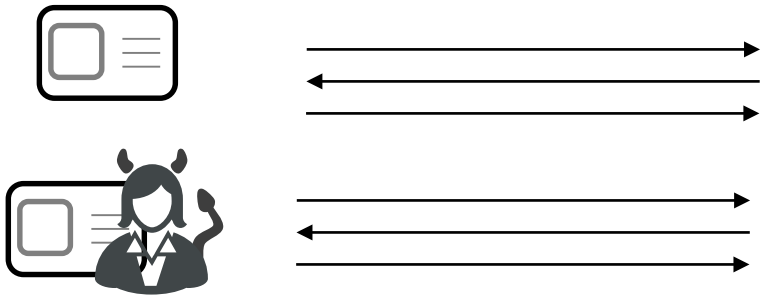
(a) → can only happen if card has also accepted with SID and A
→ adversary has only relayed data

Defining security: impersonation resistance

(a) If party accepts in session SID for partner and attributes A,
then partner also accepts SID and A in some session

(b) at most two SIDs collide, one at a card, one at a reader

Example: replay attacks



pretends to be card

accepts with SID and A

(b) →
accepts with **SID*≠SID**

(a) → can only happen if card has also accepted with SID* and A
→ adversary has only relayed data

Proving security: impersonation resistance

Theorem:

EAC with secure messaging protocol provides impersonation resistance (assuming random oracles and security of GapDH, MAC, Enc, Sig, Cert).

Proof idea:

EAC is secure key key exchange protocol [Dagdelen, Fischlin, 2010]
+
channel protocol is secure ISO/IEC 10116, ISO/IEC 9797-1 [Rogaway, 2011]

⇒ [Brzuska, 2014]

integrity of attribute transmissions

Defining security: attribute privacy

Adversary cannot distinguish betweendifferent attributes A0 and A1
used in executions between honest parties

formalized again in game-based style

Follows again from security of channel:

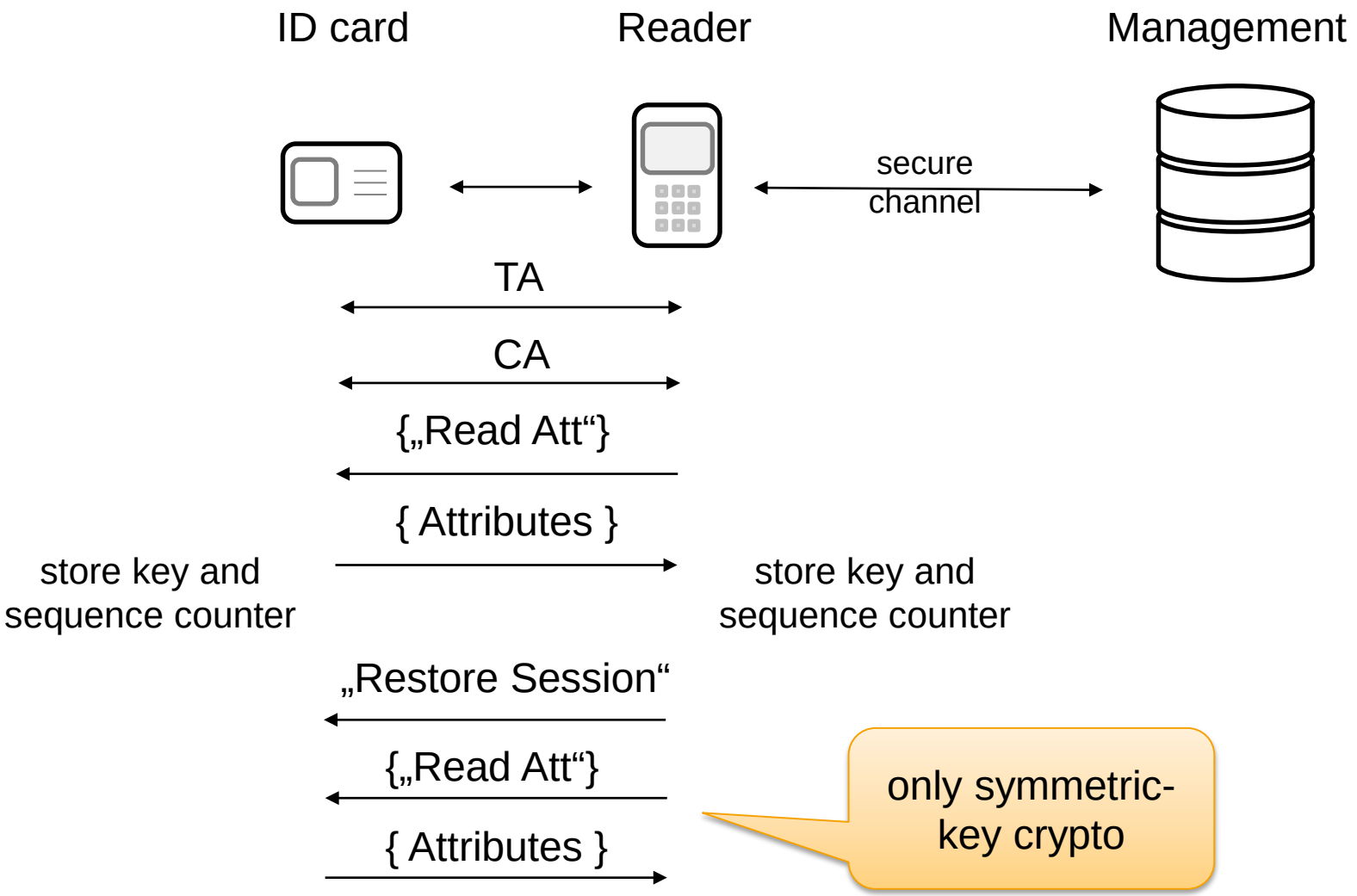
EAC is secure key key exchange protocol [Dagdelen, Fischlin, 2010]
+
channel protocol is secure ISO/IEC 10116, ISO/IEC 9797-1 [Rogaway, 2011]

⇒ [Brzuska, 2014]

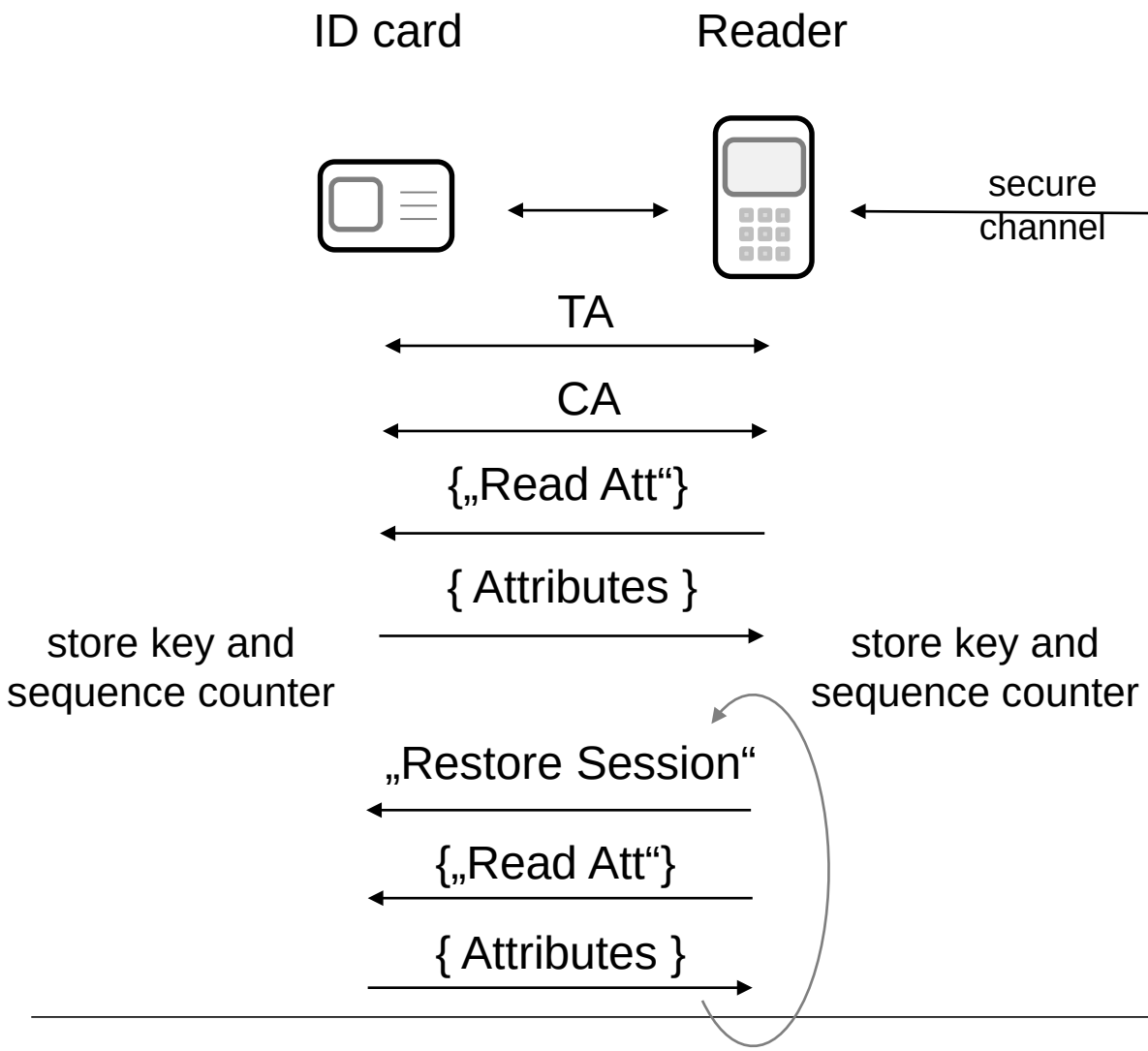
confidentiality of attribute transmissions

Restoring Sessions

Restoring sessions



Restoring sessions



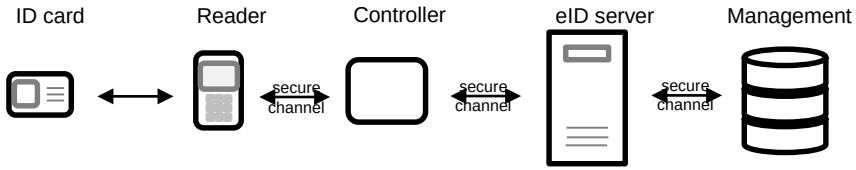
impersonation resistance + attribute privacy still guaranteed

easy to integrate via EAC‘s persistent session contexts

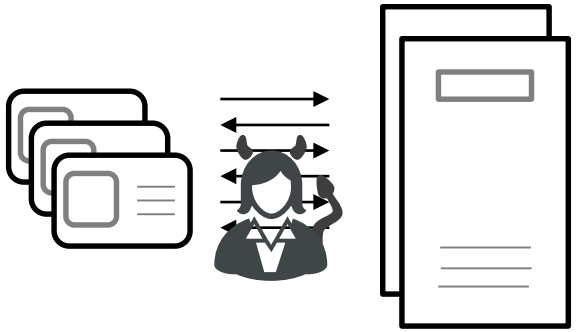
Conclusion

Conclusion

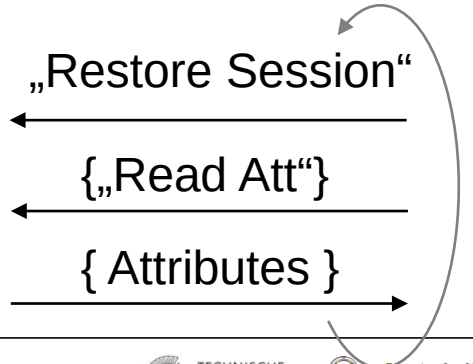
EAC protocol easy to adapt for attribute-based access control



provides strong impersonation resistance and attribute privacy



easy to restore sessions



Thank you!